


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

 Search: ☒ The ACM Digital Library ☐ The Guide



THE ACM DIGITAL LIBRARY

[Feedback](#)

cookie authentication and random numbers

 Terms used: [cookie authentication](#) [random numbers](#)

Four

 Sort results by
☒ [Save results to a Binder](#)

 Refine these results with [Ads](#)
 Try this search in [The ACM C](#)

 Display results
☐ [Open results in a new window](#)

Results 1 - 20 of 113

 Result page: 1 2 3 4 5 6 [next](#) [>>](#)

1 [End-to-end security solutions for WLAN: a performance analysis for the underlying encryption algorithms in the lightweight devices](#)

Ads



Ezedin S. Barka, Emad Eldin Mohamed, Kadhim Hayawi

July 2006 I WCMC '06: Proceedings of the 2006 international conference on Wireless communications and mobile computing

Publisher: ACM

 Full text available: pdf(235.37 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 18, Downloads (12 Months): 233, Citation Count: 0

The advances in the wireless technology, represented by the improved computational capabilities of third generation (3G) and fourth generation (4G) wireless devices and the wider bandwidth wireless networks, make it possible to support a variety of security-sensitive ...

Keyw ords: AES, J2ME, RC4, SSL/TLS, end-to-end wireless security

 C+
Pr
Ta
co
yo
Ur
Ph
Ph

 Wi
Yo
Ge
the
Pu
Op
ww

2 [The state of the art in locally distributed Web-server systems](#)



Valeria Cardellini, Emiliano Casalichio, Michele Colajanni, Philip S. Yu

June 2002 ACM Computing Surveys (CSUR), Volume 34 Issue 2

Publisher: ACM

 Full text available: pdf(1.41 MB) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 62, Downloads (12 Months): 750, Citation Count: 27

The overall increase in traffic on the World Wide Web is augmenting user-perceived response times from popular Web sites, especially in conjunction with special events. System platforms that do not replicate information content cannot provide the needed ...

Keyw ords: Client/server, World Wide Web, cluster-based architectures, dispatching algorithms, distributed systems, load balancing, routing mechanisms

 Re
Pu
Pu
an
Bo
Inv
Bo
ww

 Fri
Te
Cr
Fo
Ou
MS
De
ww

3 [COCA: A secure distributed online certification authority](#)



Lidong Zhou, Fred B. Schneider, Robbert Van Renesse

November 2002 ACM Transactions on Computer Systems (TOCS), Volume 20 Issue 4

Publisher: ACM

 Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index](#)

Full text available:  pdf(448.29 KB)

[terms](#)

Bibliometrics: Downloads (6 Weeks): 7, Downloads (12 Months): 117, Citation Count: 26

COCA is a fault-tolerant and secure online certification authority that has been built and deployed both in a local area network and in the Internet. Extremely weak assumptions characterize environments in which COCA's protocols execute correctly: no ...

Keyw ords: Byzantine quorum systems, Certification authority, denial of service, proactive secret-sharing, public key infrastructure, threshold cryptography

4 [Just fast keying: Key agreement in a hostile internet](#)



William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, Omer Reingold

May 2004 ACM Transactions on Information and System Security (TISSEC), Volume 7 Issue 2

Publisher: ACM

Full text available:  pdf(324.39 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 8, Downloads (12 Months): 156, Citation Count: 5

We describe Just Fast Keying (JFK), a new key-exchange protocol, primarily designed for use in the IP security architecture. It is simple, efficient, and secure; we sketch a proof of the latter property. JFK also has a number of novel engineering parameters ...

Keyw ords: Cryptography, denial-of-service attacks


5 [Survey of network-based defense mechanisms countering the DoS and DDoS problems](#)



Tao Peng, Christopher Leckie, Kotagiri Ramamohanarao

April 2007 ACM Computing Surveys (CSUR), Volume 39 Issue 1

Publisher: ACM

Full text available:  pdf(1.17 MB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 155, Downloads (12 Months): 2052, Citation Count: 1

This article presents a survey of denial of service attacks and the methods that have been proposed for defense against these attacks. In this survey, we analyze the design decisions in the Internet that have created the potential for denial of service ...

Keyw ords: Botnet, DDoS, DNS reflector attack, DoS, IP spoofing, IP traceback, IRC, Internet security, SYN flood, VoIP security, bandwidth attack, resource management


6 [Verified implementations of the information card federated identity-management protocol](#)



Karthikeyan Bhargavan, Cédric Fournet, Andrew D. Gordon, Nikhil Swamy

March 2008 ASI ACCS '08: Proceedings of the 2008 ACM symposium on Information, computer and communications security

Publisher: ACM

Full text available:  pdf(1.77 MB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 23, Downloads (12 Months): 57, Citation Count: 0

We describe reference implementations for selected configurations of the user authentication protocol defined by the *Information Card Profile V1.0*. Our code can interoperate with existing implementations of the roles of the protocol (client, identity ...

Keywords: CardSpace, cryptographic protocol verification, federated identity management, verified implementations, web services security

7 [Performance analysis of TLS Web servers](#)



Cristian Coarfa, Peter Druschel, Dan S. Wallach

February 2006 ACM Transactions on Computer Systems (TOCS), Volume 24 Issue 1

Publisher: ACM

Full text available: [pdf\(743.44 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#), [review](#)

Bibliometrics: Downloads (6 Weeks): 15, Downloads (12 Months): 315, Citation Count: 4

TLS is the protocol of choice for securing today's e-commerce and online transactions but adding TLS to a Web server imposes a significant overhead relative to an insecure Web server on the same platform. We perform a comprehensive study of the performance ...

Keywords: Internet, RSA accelerator, TLS, e-commerce, secure Web servers

8 [Protecting applications with transient authentication](#)



Mark D. Corner, Brian D. Noble

May 2003 MobiSys '03: Proceedings of the 1st international conference on Mobile systems, applications and services

Publisher: ACM

Full text available: [pdf\(294.40 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#)

Bibliometrics: Downloads (6 Weeks): 3, Downloads (12 Months): 92, Citation Count: 3

How does a machine know who is using it? Current systems authenticate their users infrequently, and assume the user's identity does not change. Such *persistent authentication* is inappropriate for mobile and ubiquitous systems, where associations ...

9 [Content-triggered trust negotiation](#)



Adam Hess, Jason Holt, Jared Jacobson, Kent E. Seamons

August 2004 ACM Transactions on Information and System Security (TISSEC), Volume 7 Issue 3

Publisher: ACM

Full text available: [pdf\(815.36 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 12, Downloads (12 Months): 162, Citation Count: 2

The focus of access control in client/server environments is on protecting sensitive server resources by determining whether or not a client is authorized to access those resources. The set of resources is usually static, and an access control policy ...

Keywords: Trust negotiation, access control, authentication, credentials

10 [Proceedings of the 38th SIGCSE technical symposium on Computer science education](#)



Ingrid Russell, Susan Haller, J. D. Dougherty, Susan Rodger

March 2007 proceeding

Publisher: ACM

Additional Information: [full citation](#), [abstract](#)

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Citation Count: 1

Welcome to the Northern Kentucky area and the 38th SIGCSE Technical Symposium on Computer Science Education. We are pleased to present the proceedings of SIGCSE 2007. It includes papers, panels, special sessions, posters, workshops, and birds-of-a-feather ...

11 On countering online dictionary attacks with login histories and humans-in-the-loop



Paul C. Van Oorschot, Stuart Stubblebine

August 2006 ACM Transactions on Information and System Security (TISSEC), Volume 9 Issue 3

Publisher: ACM

Full text available: pdf(305.97 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 15, Downloads (12 Months): 158, Citation Count: 1

Automated Turing Tests (ATTs), also known as human-in-the-loop techniques, were recently employed in a login protocol by Pinkas and Sander (2002) to protect against online password-guessing attacks. We present modifications providing a new history-based ...

Keyw ords: Mandatory human participation schemes, online dictionary attacks, password protocols, relay attack, usable security

12 Crypto-based identifiers (CBIDs): Concepts and applications



Gabriel Montenegro, Claude Castelluccia

February 2004 ACM Transactions on Information and System Security (TISSEC), Volume 7 Issue 1

Publisher: ACM

Full text available: pdf(262.76 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#), [review](#)

Bibliometrics: Downloads (6 Weeks): 21, Downloads (12 Months): 152, Citation Count: 3

This paper addresses the identifier ownership problem. It does so by using characteristics of Statistical Uniqueness and Cryptographic Verifiability (SUCV) of certain entities which this document calls SUCV Identifiers and Addresses, or, alternatively, ...

Keyw ords: Security, address ownership, authorization, group management, mobile IPv6, opportunistic encryption

13 Provably secure browser-based user-aware mutual authentication over TLS



Sebastian Gajek, Mark Manulis, Ahmad-Reza Sadeghi, Jörg Schwenk

March 2008 ASIACCS '08: Proceedings of the 2008 ACM symposium on Information, computer and communications security

Publisher: ACM

Full text available: pdf(410.43 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 24, Downloads (12 Months): 57, Citation Count: 0

The standard solution for user authentication on the Web is to establish a TLS-based secure channel in server authenticated mode and run a protocol on top of TLS where the user enters a password in an HTML form. However, as many studies point out, the ...

Keyw ords: TLS, browser-based protocols, phishing, user authentication

14 [Tarzan: a peer-to-peer anonymizing network layer](#)



Michael J. Freedman, Robert Morris

November 2002 CCS '02: Proceedings of the 9th ACM conference on Computer and communications security

Publisher: ACM

Full text available: pdf(242.72 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 13, Downloads (12 Months): 167, Citation Count: 30

Tarzan is a peer-to-peer anonymous IP network overlay. Because it provides IP service, Tarzan is general-purpose and transparent to applications. Organized as a decentralized peer-to-peer overlay, Tarzan is fault-tolerant, highly scalable, and easy to ...

Key words: IP tunnels, anonymity, cover traffic, distributed trust, mix-nets, overlay networks, peer-to-peer

15 [A composable framework for secure multi-modal access to internet services from Post-PC devices](#)

Steven J. Ross, Jason L. Hill, Michael Y. Chen, Anthony D. Joseph, David E. Culler, Eric A. Brewer

October 2002 Mobile Networks and Applications, Volume 7 Issue 5

Publisher: Kluwer Academic Publishers

Full text available: pdf(340.33 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#), [review](#)

Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 85, Citation Count: 1

The Post-PC revolution is bringing information access to a wide range of devices beyond the desktop, such as public kiosks, and mobile devices like cellular telephones, PDAs, and voice based vehicle telematics. However, existing deployed Internet services ...

Key words: internet, middleware, post-PC, security, transcoding

16 [Risks to the public](#)



Peter G. Neumann

July 2005 ACM SIGSOFT Software Engineering Notes, Volume 30 Issue 4

Publisher: ACM

Full text available: pdf(151.77 KB) Additional Information: [full citation](#), [abstract](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 24, Downloads (12 Months): 306, Citation Count: 0

Edited by Peter G. Neumann (Risks Forum Moderator and Chairman of the ACM Committee on Computers and Public Policy), plus personal contributions by others, as indicated. Opinions expressed are individual rather than organizational, and all of the usual ...

17 [Structured streams: a new transport abstraction](#)



Bryan Ford

August 2007 SIGCOMM '07: Proceedings of the 2007 conference on Applications, technologies, architectures, and protocols for computer communications

Publisher: ACM

Full text available: pdf(694.68 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 12, Downloads (12 Months): 284, Citation Count: 1

Internet applications currently have a choice between stream and datagram transport abstractions. Datagrams efficiently support small transactions and streams are suited for long-running conversations, but neither abstraction adequately supports applications ...

Keywords: SST, TCP, best-effort, datagram, fairness, mobility, multimedia, reliable, stream, transport protocols, web transport

18 [Structured streams: a new transport abstraction](#)



Bryan Ford

October 2007 ACM SIGCOMM Computer Communication Review, Volume 37 Issue 4

Publisher: ACM

Full text available: pdf(694.88 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 12, Downloads (12 Months): 284, Citation Count: 1

Internet applications currently have a choice between stream and datagram transport abstractions. Datagrams efficiently support small transactions and streams are suited for long-running conversations, but neither abstraction adequately supports applications ...

Keywords: SST, TCP, best-effort, datagram, fairness, mobility, multimedia, reliable, stream, transport protocols, web transport

19 [Efficient, DoS-resistant, secure key exchange for internet protocols](#)



William Aiello, Steven M. Bellovin, Matt Blaze, John Ioannidis, Omer Reingold, Ran Canetti, Angelos D. Keromytis

November 2002 CCS '02: Proceedings of the 9th ACM conference on Computer and communications security

Publisher: ACM

Full text available: pdf(118.52 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 12, Downloads (12 Months): 110, Citation Count: 15

We describe JFK, a new key exchange protocol, primarily designed for use in the IP Security Architecture. It is simple, efficient, and secure; we sketch a proof of the latter property. JFK also has a number of novel engineering parameters that permit ...

Keywords: cryptography, denial of service attacks

20 [Some Trends in Web Application Development](#)

Mehdi Jazayeri

May 2007 FOSE '07: 2007 Future of Software Engineering

Publisher: IEEE Computer Society

Full text available: pdf(172.29 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 24, Downloads (12 Months): 1640, Citation Count: 2





A Web application is an application that is invoked with a Web browser over the Internet. Ever since 1994 when the Internet became available to the public and especially in 1995 when the World Wide Web put a usable face on the Internet, the Internet ...

Results 1 - 20 of 113

Result page: 1 2 3 4 5 6 next >>

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2008 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)